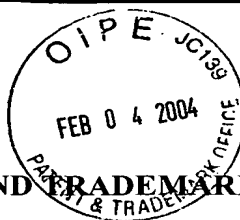


Docket No. 242743US2/ims



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Tsutomu OHISHI, et al.

GAU: 2185

SERIAL NO: 10/660,698

EXAMINER:

FILED: September 12, 2003

FOR: IMAGE FORMING APPARATUS AND USE CONTROL METHOD

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS  
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e): Application No. Date Filed

- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
JAPAN	2002-269285	September 13, 2002
JAPAN	2003-318476	September 10, 2003
JAPAN	2003-318477	September 10, 2003

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number  
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- ☐ (B) Application Serial No.(s)
- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.

Marvin J. Spivak

Registration No. 24,913

Joseph A. Scafetta, Jr.  
Registration No. 26, 803

Customer Number

22850

Tel. (703) 413-3000  
Fax. (703) 413-2220  
(OSMMN 05/03)

101660, 698

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日            2 0 0 2 年    9 月 1 3 日  
Date of Application:

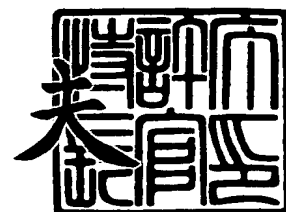
出 願 番 号            特 願 2 0 0 2 - 2 6 9 2 8 5  
Application Number:  
[ST. 10/C] :            [ J P 2 0 0 2 - 2 6 9 2 8 5 ]

出      願      人            株 式 会 社 リ コ ー  
Applicant(s):

2 0 0 3 年    8 月 1 1 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康



出証番号    出証特 2 0 0 3 - 3 0 6 4 2 1 7

【書類名】 特許願

【整理番号】 0204747

【提出日】 平成14年 9月13日

【あて先】 特許庁長官殿

【国際特許分類】 G03G 21/00 370

【発明の名称】 画像形成装置、利用者認証方法および課金処理方法

【請求項の数】 16

【発明者】

    【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内

    【氏名】 大石 勉

【発明者】

    【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内

    【氏名】 中川 克彦

【特許出願人】

    【識別番号】 000006747

    【氏名又は名称】 株式会社リコー

【代理人】

    【識別番号】 100089118

    【弁理士】

    【氏名又は名称】 酒井 宏明

【手数料の表示】

    【予納台帳番号】 036711

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

    【包括委任状番号】 9808514

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 画像形成装置、利用者認証方法および課金処理方法

【特許請求の範囲】

【請求項 1】 画像形成処理にかかるユーザサービスを提供する画像形成装置であって、

利用者に固有の利用者識別情報と、利用者の正当性を示す利用者認証情報を入力させる利用者情報入力処理手段と、

ネットワークに接続され、前記利用者識別情報と前記利用者認証情報を管理する外部サーバに対し、前記利用者情報入力処理手段によって入力された利用者識別情報を送信し、外部サーバによって前記利用者識別情報に基づいて検索された利用者認証情報を受信する外部サーバ通信手段と、

前記外部サーバ通信手段によって受信した利用者認証情報と、前記利用者情報入力処理手段によって入力された利用者認証情報とが一致するか否かを判断し、判断結果を、画像形成装置で動作する他のプロセスに通知する認証手段と、

を備えたことを特徴とする画像形成装置。

【請求項 2】 前記認証手段による判断結果に基づいて、画像形成装置の利用制限を行う利用制限手段をさらに備え、

前記認証手段は、前記判断結果を、前記利用制限手段に通知することを特徴とする請求項 1 に記載の画像形成装置。

【請求項 3】 前記外部サーバ通信手段は、前記利用者識別情報と前記利用者認証情報を管理するインターネット上の LDAP (Lightweight Directory Access Protocol) サーバに対し、前記利用者情報入力処理手段によって入力された利用者識別情報を送信し、前記 LDAP サーバによって前記利用者識別情報に基づいて検索された利用者認証情報を受信することを特徴とする請求項 1 または 2 に記載の画像形成装置。

【請求項 4】 画像形成処理で使用されるハードウェア資源と、

画像形成処理にかかるユーザサービスにそれぞれ固有の処理を行うアプリケーションと、

前記アプリケーションと前記ハードウェア資源との間に介在し、ユーザサービ

スを提供する際に、アプリケーションの少なくとも2つが共通的に必要とする前記ハードウェア資源の獲得要求、管理、実行制御並びに画像形成処理を行うコントロールサービスと、をさらに備え、

前記アプリケーションは、前記利用者情報入力処理手段、前記外部サーバ通信手段および前記認証手段前記通知手段として動作する認証アプリを備え、

前記コントロールサービスは、前記利用制限手段として動作する認証コントロールサービスを備えたことを特徴とする請求項2または3に記載の画像形成装置。

【請求項5】 画像形成処理にかかるユーザサービスを提供する画像形成装置であって、

利用者に固有の利用者識別情報と、利用者による画像形成装置の使用状況を示す課金情報とを、ネットワークに接続されたクライアント端末から受信する利用者情報受信手段と、

前記利用者情報受信手段によって前記利用者識別情報と前記課金情報を受信したときに、前記ネットワークに接続され、前記利用者識別情報と前記課金情報とを管理する外部サーバに対し、前記利用者情報受信手段によって受信した前記利用者識別情報を送信し、外部サーバによって前記利用者識別情報に基づいて検索された課金情報を受信する外部サーバ通信手段と、

前記外部サーバ通信手段によって受信した課金情報と、前記利用者情報受信手段によって受信した課金情報とを比較し、比較結果を画像形成装置で動作する他のプロセスに通知する課金処理手段と、

を備えたことを特徴とする画像形成装置。

【請求項6】 前記課金情報に基づいて、画像形成装置の利用者の利用制限を行う利用制限手段をさらに備え、

前記課金処理手段は、前記比較結果を、前記利用制限手段に通知することを特徴とする請求項5に記載の画像形成装置。

【請求項7】 前記利用者情報受信手段は、前記クライアント端末が外部記憶媒体から読み出した前記利用者識別情報と前記課金情報を、前記クライアント端末から受信することを特徴とする請求項5または6に記載の画像形成装置。

【請求項 8】 前記外部サーバ通信手段は、前記利用者識別情報と前記利用者認証情報を管理するインターネット上の LDAP (Lightweight Directory Access Protocol) サーバに対し、前記利用者情報入力処理手段によって入力された利用者識別情報を送信し、前記 LDAP サーバによって前記利用者識別情報に基づいて検索された前記課金情報を受信することを特徴とする請求項 5～7 のいずれか一つに記載の画像形成装置。

【請求項 9】 画像形成処理で使用されるハードウェア資源と、  
画像形成処理にかかるユーザサービスにそれぞれ固有の処理を行うアプリケーションと、

前記アプリケーションと前記ハードウェア資源との間に介在し、ユーザサービスを提供する際に、アプリケーションの少なくとも 2 つが共通的に必要とする前記ハードウェア資源の獲得要求、管理、実行制御並びに画像形成処理を行うコントロールサービスと、をさらに備え、

前記アプリケーションは、前記利用者情報受信手段、前記外部サーバ通信手段および前記課金処理手段として動作する課金アプリを備え、

前記コントロールサービスは、前記利用制限手段として動作する認証コントロールサービスを備えたことを特徴とする請求項 6～8 のいずれか一つに記載の画像形成装置。

【請求項 10】 画像形成処理にかかるユーザサービスを提供する画像形成装置の利用者の認証処理を行う利用者認証方法であって、

利用者に固有の利用者識別情報と、利用者の正当性を示す利用者認証情報を入力させる利用者情報入力処理ステップと、

ネットワークに接続され、前記利用者識別情報と前記利用者認証情報を管理する外部サーバに対し、前記利用者情報入力処理ステップによって入力された利用者識別情報を送信し、外部サーバによって前記利用者識別情報に基づいて検索された利用者認証情報を受信する外部サーバ通信ステップと、

前記外部サーバ通信ステップによって受信した利用者認証情報と、前記利用者情報入力処理ステップによって入力された利用者認証情報とが一致するか否かを判断し、判断結果を、画像形成装置で動作する他のプロセスに通知する認証ステ

ップと、

を含むことを特徴とする利用者認証方法。

【請求項 11】 前記認証ステップによる判断結果に基づいて、画像形成装置の利用制限を行う利用制限ステップをさらに備え、

前記認証ステップは、前記判断結果を、前記利用制限ステップを実行するプロセスに通知することを特徴とする請求項 10 に記載の利用者認証方法。

【請求項 12】 前記外部サーバ通信ステップは、前記利用者識別情報と前記利用者認証情報を管理するインターネット上の LDAP サーバに対し、前記利用者情報入力処理ステップによって入力された利用者識別情報を送信し、前記 LDAP サーバによって前記利用者識別情報に基づいて検索された利用者認証情報を受信することを特徴とする請求項 10 または 11 に記載の利用者認証方法。

【請求項 13】 画像形成処理にかかるユーザサービスを提供する画像形成装置の利用者の課金処理を行う課金処理方法であって、

利用者に固有の利用者識別情報と、利用者による画像形成装置の使用状況を示す課金情報とを、ネットワークに接続されたクライアント端末から受信する利用者情報受信ステップと、

前記利用者情報受信ステップによって前記利用者識別情報と前記課金情報を受信したときに、前記ネットワークに接続され、前記利用者識別情報と前記課金情報とを管理する外部サーバに対し、前記利用者情報受信ステップによって受信した前記利用者識別情報を送信し、外部サーバによって前記利用者識別情報に基づいて検索された課金情報を受信する外部サーバ通信ステップと、

前記外部サーバ通信ステップによって受信した課金情報と、前記利用者情報受信ステップによって受信した課金情報とを比較し、比較結果を画像形成装置で動作する他のプロセスに通知する課金処理ステップと、

を含むことを特徴とする課金処理方法。

【請求項 14】 前記課金情報に基づいて、画像形成装置の利用者の利用制限を行う利用制限ステップをさらに備え、

前記課金処理ステップは、前記比較結果を、前記利用制限ステップを実行するプロセスに通知することを特徴とする請求項 13 に記載の課金処理方法。

【請求項 15】 前記利用者情報受信ステップは、前記クライアント端末が外部記憶媒体から読み出した前記利用者識別情報と前記課金情報を、前記クライアント端末から受信することを特徴とする請求項 13 または 14 に記載の課金処理方法。

【請求項 16】 前記外部サーバ通信ステップは、前記利用者識別情報と前記利用者認証情報を管理するインターネット上の LDAP サーバに対し、前記利用者情報入力処理ステップによって入力された利用者識別情報を送信し、前記 LDAP サーバによって前記利用者識別情報に基づいて検索された前記課金情報を受信することを特徴とする請求項 13～15 のいずれか一つに記載の課金処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、コピー、プリンタ、スキャナ、ファクシミリなどの画像形成処理にかかるユーザサービスを提供し、利用者の認証処理や課金処理をネットワークに接続された外部サーバを利用して行うことができる画像形成装置、利用者認証方法および課金処理方法に関するものである。

【0002】

【従来の技術】

近年では、プリンタ、コピー、ファクシミリ、スキャナなどの各装置の機能を 1 つの筐体内に収納した画像形成装置（以下、「複合機」という。）が知られている。この複合機は、1 つの筐体内に表示部、印刷部および撮像部などを設けるとともに、プリンタ、コピーおよびファクシミリ装置にそれぞれ対応した 3 種類のソフトウェアを設け、これらのソフトウェアを切り替えることによって、当該装置をプリンタ、コピー、スキャナまたはファクシミリ装置として動作させるものである。

【0003】

ところで、このような従来の複合機では、プリンタ、コピー、スキャナおよびファクシミリ装置に対応するソフトウェアをそれぞれ別個に設けているため、各



ソフトウェアの開発に多大の時間を要する。このため、出願人は、表示部、印刷部および撮像部などの画像形成処理で使用するハードウェア資源を有し、プリンタ、コピーまたはファクシミリなどの各ユーザサービスにそれぞれ固有の処理を行うアプリケーションを複数搭載し、これらのアプリケーションとハードウェア資源との間に介在して、ユーザサービスを提供する際に、アプリケーションの少なくとも2つが共通的に必要とするハードウェア資源の管理、実行制御並びに画像形成処理を行う各種コントロールサービスからなるプラットフォームを含む画像形成装置（複合機）を発明した。

#### 【0004】

このような複合機では、利用者が複合機を利用する際にユーザIDとパスワードなどによる利用者認証を行い、複合機の不正な利用者による利用を制限したり、利用者の課金情報に基づいて利用制限を行ってセキュリティ面の強化を図っているものがある。このような認証機能および課金機能を備えた複合機では、一般的に、ユーザIDとパスワードを自己の記憶装置内の認証データベースで管理し、ユーザIDと課金情報を自己の記憶装置内の課金データベースすることが一般的となっている。特に、近年、複合機の使用形態としては、LAN（Local Area Network）やインターネットなどのネットワークに複数の複合機あるいはプリンタ装置を接続し、ネットワーク上のPC（Personal Computer）やワークステーションなどのコンピュータから利用するというものが一般的となっている。このため、ネットワークに接続された複合機ごとに認証データベースや課金データベースを設け、各複合機を利用可能な利用者のユーザIDおよびパスワードを管理する必要がある。

#### 【0005】

##### 【発明が解決しようとする課題】

しかしながら、このようなユーザIDやパスワードなどの認証情報や課金情報を、自己の複合機内の認証データベースあるいは課金データベースで管理する場合、ネットワークに接続された個々の複合機ごとに認証データベースおよび課金データベースを設けて、それぞれ別個に管理しなければならないため、認証情報や課金情報の管理が煩雑になるという問題がある。

## 【0006】

すなわち、ネットワーク上の個々の複合機について、各複合機ごとに利用可能な利用者と利用不可能な利用者が異なる場合が考えられるため、利用者の固有の情報や認証情報あるいは課金情報を更新する場合に、どの複合機で利用可能な利用者かを判断しなければならず、ネットワーク上に多数の複合機が接続されている場合には、認証情報や課金情報の管理労力が増大する。また、複合機のシステム管理者以外に認証情報の追加、変更、削除などの認証データベースの更新、あるいは課金データベースの更新が制限されている場合でも、一人の利用者の認証情報または課金情報に変更がある場合、ネットワーク上のすべての複合機の認証データベースおよび課金データベースの更新が必要となるため、複合機ごとにシステム管理者が異なれば、認証情報や課金情報のメンテナンス作業の労力が膨大なものとなる。

## 【0007】

また、ネットワーク上の各複合機ごとに認証データベース、課金データベースを管理する場合には、認証データベースの更新を複合機のシステム管理者のみに制限している場合であっても、利用者のシステム管理者のなりすましによって、パスワードを変更するなどの認証データベースや課金データベースを不正に改ざんすることが容易に可能となってしまう、セキュリティ面の脆弱性が問題となる。

## 【0008】

この発明は上記に鑑みてなされたもので、利用者の認証情報や課金情報など利用者情報をネットワーク上の外部サーバを利用して一括管理することによって、利用者情報のメンテナンス作業の労力を軽減するとともに、利用者情報のセキュリティの強化を図ることができる画像形成装置、利用者認証方法および課金処理方法を得ることを目的とする。

## 【0009】

## 【課題を解決するための手段】

上記目的を達成するため、請求項1にかかる発明は、画像形成処理にかかるユーザサービスを提供する画像形成装置であって、利用者に固有の利用者識別情報

と、利用者の正当性を示す利用者認証情報を入力させる利用者情報入力処理手段と、ネットワークに接続され、前記利用者識別情報と前記利用者認証情報を管理する外部サーバに対し、前記利用者情報入力処理手段によって入力された利用者識別情報を送信し、外部サーバによって前記利用者識別情報に基づいて検索された利用者認証情報を受信する外部サーバ通信手段と、前記外部サーバ通信手段によって受信した利用者認証情報と、前記利用者情報入力処理手段によって入力された利用者認証情報とが一致するか否かを判断し、判断結果を、画像形成装置で動作する他のプロセスに通知する認証手段と、を備えたことを特徴とする。

#### 【0010】

この請求項1にかかる発明によれば、利用者情報入力処理手段によって、利用者に固有の利用者識別情報と利用者の正当性を示す利用者認証情報を入力させ、外部サーバ通信手段によって、ネットワークに接続され利用者識別情報と利用者認証情報を管理する外部サーバに対し利用者情報入力処理手段によって入力された利用者識別情報を送信し、外部サーバによって利用者識別情報に基づいて検索された利用者認証情報を受信し、認証手段によって、外部サーバ通信手段によって受信した利用者認証情報と、利用者情報入力処理手段によって入力された利用者認証情報とが一致するか否かを判断し、判断結果を、画像形成装置で動作する他のプロセスに通知することで、外部サーバで利用者識別情報と利用者認証情報とを一括管理するので、自己の画像形成装置内に利用者識別情報と利用者認証情報とを対応づけた認証データベースを保持する必要がなくなり、認証データベースのメンテナンス作業の労力を軽減することができる。また、各画像形成装置に認証データベースを保持する必要がないため、利用者認証情報の改ざんを防止することができ、画像形成装置のセキュリティの強化を図ることができる。

#### 【0011】

また、請求項2にかかる発明は、請求項1に記載の画像形成装置において、前記認証手段による判断結果に基づいて、画像形成装置の利用制限を行う利用制限手段をさらに備え、前記認証手段は、前記判断結果を、前記利用制限手段に通知することを特徴とする。

#### 【0012】

この請求項 2 にかかる発明によれば、認証手段によって、判断結果を利用制限手段に通知し、利用制限手段によって、認証手段による判断結果に基づいて画像形成装置の利用制限を行うことで、認証データベースのメンテナンス作業の労力の軽減を図りつつ、利用者認証情報に基づく画像形成装置の利用制限によるセキュリティ強化を向上させることができる。

【0013】

また、請求項 3 にかかる発明は、請求項 1 または 2 に記載の画像形成装置において、前記外部サーバ通信手段は、前記利用者識別情報と前記利用者認証情報を管理するインターネット上の LDAP サーバに対し、前記利用者情報入力処理手段によって入力された利用者識別情報を送信し、前記 LDAP サーバによって前記利用者識別情報に基づいて検索された利用者認証情報を受信することを特徴とする。

【0014】

この請求項 3 にかかる発明によれば、外部サーバ通信手段によって、利用者識別情報と利用者認証情報を管理するインターネット上の LDAP サーバに対し、利用者情報入力処理手段によって入力された利用者識別情報を送信し、LDAP サーバによって利用者識別情報に基づいて検索された利用者認証情報を受信することで、利用者認証情報の検索時間を短縮することができる。

【0015】

また、請求項 4 にかかる発明は、請求項 2 または 3 に記載の画像形成装置において、画像形成処理で使用されるハードウェア資源と、画像形成処理にかかるユーザサービスにそれぞれ固有の処理を行うアプリケーションと、前記アプリケーションと前記ハードウェア資源との間に介在し、ユーザサービスを提供する際に、アプリケーションの少なくとも 2 つが共通的に必要とする前記ハードウェア資源の獲得要求、管理、実行制御並びに画像形成処理を行うコントロールサービスと、をさらに備え、前記アプリケーションは、前記利用者情報入力処理手段、前記外部サーバ通信手段および前記認証手段前記通知手段として動作する認証アプリを備え、前記コントロールサービスは、前記利用制限手段として動作する認証コントロールサービスを備えたことを特徴とする。

## 【0016】

この請求項4にかかる発明によれば、画像形成処理で使用するハードウェア資源と、画像形成処理にかかるユーザサービスにそれぞれ固有の処理を行うアプリケーションと、前記アプリケーションと前記ハードウェア資源との間に介在し、ユーザサービスを提供する際に、アプリケーションの少なくとも2つが共通的に必要とする前記ハードウェア資源の獲得要求、管理、実行制御並びに画像形成処理を行うコントロールサービスと、をさらに備え、前記アプリケーションは、前記利用者情報入力処理手段、前記外部サーバ通信手段および前記認証手段前記通知手段として動作する認証アプリを備え、前記コントロールサービスは、前記利用制限手段として動作する認証コントロールサービスを備えたので、認証アプリをはじめとするアプリケーションのソフトウェア開発において、ユーザサービスに固有の部分だけで行うことができ、ソフトウェア開発の労力軽減を図ることができる。

## 【0017】

また、請求項5にかかる発明は、画像形成処理にかかるユーザサービスを提供する画像形成装置であって、利用者に固有の利用者識別情報と、利用者による画像形成装置の使用状況を示す課金情報とを、ネットワークに接続されたクライアント端末から受信する利用者情報受信手段と、前記利用者情報受信手段によって前記利用者識別情報と前記課金情報を受信したときに、前記ネットワークに接続され、前記利用者識別情報と前記課金情報とを管理する外部サーバに対し、前記利用者情報受信手段によって受信した前記利用者識別情報を送信し、外部サーバによって前記利用者識別情報に基づいて検索された課金情報を受信する外部サーバ通信手段と、前記外部サーバ通信手段によって受信した課金情報と、前記利用者情報受信手段によって受信した課金情報とを比較し、比較結果を画像形成装置で動作する他のプロセスに通知する課金処理手段と、を備えた。

## 【0018】

この請求項5にかかる発明によれば、利用者情報受信手段によって、利用者に固有の利用者識別情報と、利用者による画像形成装置の使用状況を示す課金情報とを、ネットワークに接続されたクライアント端末から受信し、外部サーバ通信

手段によって、利用者情報受信手段によって利用者識別情報と課金情報を受信したときに、ネットワークに接続され、利用者識別情報と課金情報とを管理する外部サーバに対し、利用者情報受信手段によって受信した利用者識別情報を送信し、外部サーバによって利用者識別情報に基づいて検索された課金情報を受信し、課金処理手段によって、外部サーバ通信手段によって受信した課金情報と、利用者情報受信手段によって受信した課金情報とを比較し、比較結果を画像形成装置で動作する他のプロセスに通知することで、外部サーバで利用者識別情報と課金情報とを一括管理するので、自己の画像形成装置内に利用者識別情報と課金情報とを対応づけた課金データベースを保持する必要がなくなり、課金データベースのメンテナンス作業の労力を軽減することができる。また、各画像形成装置に課金データベースを保持する必要がないため、課金情報の改ざんを防止することができ、画像形成装置のセキュリティの強化を図ることができる。

#### 【0019】

また、請求項6にかかる発明は、請求項5に記載の画像形成装置において、前記課金情報に基づいて、画像形成装置の利用者の利用制限を行う利用制限手段をさらに備え、前記課金処理手段は、前記比較結果を、前記利用制限手段に通知することを特徴とする。

#### 【0020】

この請求項6にかかる発明によれば、課金処理手段によって、比較結果を利用制限手段に通知し、利用制限手段によって、課金情報に基づいて、画像形成装置の利用者の利用制限を行うことで、課金データベースのメンテナンス作業の労力の軽減を図りつつ、課金情報に基づく画像形成装置の利用制限によるセキュリティ強化を向上させることができる。

#### 【0021】

また、請求項7にかかる発明は、請求項5または6に記載の画像形成装置において、前記利用者情報受信手段は、前記クライアント端末が外部記憶媒体から読み出した前記利用者識別情報と前記課金情報を、前記クライアント端末から受信することを特徴とする。

#### 【0022】

この請求項7にかかる発明によれば、利用者情報受信手段によって、クライアント端末が外部記憶媒体から読み出した利用者識別情報と課金情報を、クライアント端末から受信することで、任意の外部記憶媒体に記録した課金情報に基づく利用制限を行うことができ、利用者の便宜が図られる。

#### 【0023】

また、請求項8にかかる発明は、請求項5～7のいずれか一つに記載の画像形成装置において、前記外部サーバ通信手段は、前記利用者識別情報と前記利用者認証情報を管理するインターネット上のLDAP (Lightweight Directory Access Protocol) サーバに対し、前記利用者情報入力処理手段によって入力された利用者識別情報を送信し、前記LDAPサーバによって前記利用者識別情報に基づいて検索された前記課金情報を受信することを特徴とする。

#### 【0024】

この請求項8にかかる発明によれば、外部サーバ通信手段によって、利用者識別情報と利用者認証情報を管理するインターネット上のLDAPサーバに対し、利用者情報入力処理手段によって入力された利用者識別情報を送信し、LDAPサーバによって利用者識別情報に基づいて検索された課金情報を受信することで、課金情報の検索時間を短縮することができる。

#### 【0025】

また、請求項9にかかる発明は、請求項6～8のいずれか一つに記載の画像形成装置において、画像形成処理で使用されるハードウェア資源と、画像形成処理にかかるユーザサービスにそれぞれ固有の処理を行うアプリケーションと、前記アプリケーションと前記ハードウェア資源との間に介在し、ユーザサービスを提供する際に、アプリケーションの少なくとも2つが共通的に必要とする前記ハードウェア資源の獲得要求、管理、実行制御並びに画像形成処理を行うコントロールサービスと、をさらに備え、前記アプリケーションは、前記利用者情報受信手段、前記外部サーバ通信手段および前記課金処理手段として動作する認証アプリを備え、前記コントロールサービスは、前記利用制限手段として動作する認証コントロールサービスを備えたことを特徴とする。

## 【0026】

この請求項9にかかる発明によれば、画像形成処理で使用されるハードウェア資源と、画像形成処理にかかるユーザサービスにそれぞれ固有の処理を行うアプリケーションと、アプリケーションとハードウェア資源との間に介在し、ユーザサービスを提供する際に、アプリケーションの少なくとも2つが共通的に必要とするハードウェア資源の獲得要求、管理、実行制御並びに画像形成処理を行うコントロールサービスと、をさらに備え、アプリケーションは、利用者情報受信手段、外部サーバ通信手段および課金処理手段として動作する課金アプリを備え、コントロールサービスは、利用制限手段として動作する認証コントロールサービスを備えたので、課金アプリをはじめとするアプリケーションのソフトウェア開発において、ユーザサービスに固有の部分だけで行うことができ、ソフトウェア開発の労力軽減を図ることができる。

## 【0027】

また、請求項10にかかる発明は、画像形成処理にかかるユーザサービスを提供する画像形成装置の利用者の認証処理を行う利用者認証方法であって、利用者に固有の利用者識別情報と、利用者の正当性を示す利用者認証情報を入力させる利用者情報入力処理ステップと、ネットワークに接続され、前記利用者識別情報と前記利用者認証情報を管理する外部サーバに対し、前記利用者情報入力処理ステップによって入力された利用者識別情報を送信し、外部サーバによって前記利用者識別情報に基づいて検索された利用者認証情報を受信する外部サーバ通信ステップと、前記外部サーバ通信ステップによって受信した利用者認証情報と、前記利用者情報入力処理ステップによって入力された利用者認証情報とが一致するか否かを判断し、判断結果を、画像形成装置で動作する他のプロセスに通知する認証ステップと、を含むことを特徴とする。

## 【0028】

この請求項10にかかる発明によれば、利用者情報入力処理ステップによって、利用者に固有の利用者識別情報と利用者の正当性を示す利用者認証情報を入力させ、外部サーバ通信ステップによって、ネットワークに接続され利用者識別情報と利用者認証情報を管理する外部サーバに対し利用者情報入力処理ステップに



よって入力された利用者識別情報を送信し、外部サーバによって利用者識別情報に基づいて検索された利用者認証情報を受信し、認証ステップによって、外部サーバ通信ステップによって受信した利用者認証情報と、利用者情報入力処理ステップによって入力された利用者認証情報とが一致するか否かを判断し、判断結果を、画像形成装置で動作する他のプロセスに通知することで、外部サーバで利用者識別情報と利用者認証情報とを一括管理するので、自己の画像形成装置内に利用者識別情報と利用者認証情報とを対応づけた認証データベースを保持する必要がなくなり、認証データベースのメンテナンス作業の労力を軽減することができる。また、各画像形成装置に認証データベースを保持する必要がないため、利用者認証情報の改ざんを防止することができ、画像形成装置のセキュリティの強化を図ることができる。

#### 【0029】

また、請求項11にかかる発明は、請求項10に記載の利用者認証方法において、前記認証ステップによる判断結果に基づいて、画像形成装置の利用制限を行う利用制限ステップをさらに備え、前記認証ステップは、前記判断結果を、前記利用制限ステップを実行するプロセスに通知することを特徴とする。

#### 【0030】

この請求項11にかかる発明によれば、利用制限ステップによって、認証ステップによる判断結果に基づいて、画像形成装置の利用制限を行い、認証ステップは、判断結果を利用制限ステップを実行するプロセスに通知することで、認証データベースのメンテナンス作業の労力の軽減を図りつつ、利用者認証情報に基づく画像形成装置の利用制限によるセキュリティ強化を向上させることができる。

#### 【0031】

また、請求項12にかかる発明は、請求項10または11に記載の利用者認証方法において、前記外部サーバ通信ステップは、前記利用者識別情報と前記利用者認証情報を管理するインターネット上のLDAPサーバに対し、前記利用者情報入力処理ステップによって入力された利用者識別情報を送信し、前記LDAPサーバによって前記利用者識別情報に基づいて検索された利用者認証情報を受信することを特徴とする。

## 【 0 0 3 2 】

この請求項 1 2 にかかる発明によれば、外部サーバ通信ステップによって、利用者識別情報と利用者認証情報を管理するインターネット上の L D A P サーバに対し、利用者情報入力処理ステップによって入力された利用者識別情報を送信し、L D A P サーバによって利用者識別情報に基づいて検索された利用者認証情報を受信することで、利用者認証情報の検索時間を短縮することができる。

## 【 0 0 3 3 】

また、請求項 1 3 にかかる発明は、画像形成処理にかかるユーザサービスを提供する画像形成装置の利用者の課金処理を行う課金処理方法であって、利用者に固有の利用者識別情報と、利用者による画像形成装置の使用状況を示す課金情報とを、ネットワークに接続されたクライアント端末から受信する利用者情報受信ステップと、前記利用者情報受信ステップによって前記利用者識別情報と前記課金情報を受信したときに、前記ネットワークに接続され、前記利用者識別情報と前記課金情報とを管理する外部サーバに対し、前記利用者情報受信ステップによって受信した前記利用者識別情報を送信し、外部サーバによって前記利用者識別情報に基づいて検索された課金情報を受信する外部サーバ通信ステップと、前記外部サーバ通信ステップによって受信した課金情報と、前記利用者情報受信ステップによって受信した課金情報とを比較し、比較結果を画像形成装置で動作する他のプロセスに通知する課金処理ステップと、を含むことを特徴とする。

## 【 0 0 3 4 】

この請求項 1 3 にかかる発明によれば、利用者情報受信ステップによって、利用者に固有の利用者識別情報と、利用者による画像形成装置の使用状況を示す課金情報とを、ネットワークに接続されたクライアント端末から受信し、外部サーバ通信ステップによって、利用者情報受信ステップによって利用者識別情報と課金情報を受信したときに、ネットワークに接続され、利用者識別情報と課金情報とを管理する外部サーバに対し、利用者情報受信ステップによって受信した利用者識別情報を送信し、外部サーバによって利用者識別情報に基づいて検索された課金情報を受信し、課金処理ステップによって、外部サーバ通信ステップによって受信した課金情報と、利用者情報受信ステップによって受信した課金情報とを

比較し、比較結果を画像形成装置で動作する他のプロセスに通知することで、外部サーバで利用者識別情報と課金情報とを一括管理するので、自己の画像形成装置内に利用者識別情報と課金情報とを対応づけた課金データベースを保持する必要がなくなり、課金データベースのメンテナンス作業の労力を軽減することができる。また、各画像形成装置に課金データベースを保持する必要がないため、課金情報の改ざんを防止することができ、画像形成装置のセキュリティの強化を図ることができる。

#### 【0035】

また、請求項14にかかる発明は、請求項13に記載の課金処理方法において、前記課金情報に基づいて、画像形成装置の利用者の利用制限を行う利用制限ステップをさらに備え、前記課金処理ステップは、前記比較結果を、前記利用制限ステップを実行するプロセスに通知することを特徴とする。

#### 【0036】

この請求項14にかかる発明によれば、利用制限ステップによって、課金情報に基づいて、画像形成装置の利用者の利用制限を行い、課金処理ステップによって、比較結果を利用制限ステップを実行するプロセスに通知することで、課金データベースのメンテナンス作業の労力の軽減を図りつつ、課金情報に基づく画像形成装置の利用制限によるセキュリティ強化を向上させることができる。

#### 【0037】

また、請求項15にかかる発明は、請求項13または14に記載の課金処理方法において、前記利用者情報受信ステップは、前記クライアント端末が外部記憶媒体から読み出した前記利用者識別情報と前記課金情報を、前記クライアント端末から受信することを特徴とする。

#### 【0038】

この請求項15にかかる発明によれば、利用者情報受信ステップによって、クライアント端末が外部記憶媒体から読み出した利用者識別情報と課金情報を、前記クライアント端末から受信することで、任意の外部記憶媒体に記録した課金情報に基づく利用制限を行うことができ、利用者の便宜が図られる。

#### 【0039】

また、請求項 16 にかかる発明は、請求項 13～15 のいずれか一つに記載の課金処理方法において、前記外部サーバ通信ステップは、前記利用者識別情報と前記利用者認証情報を管理するインターネット上の LDAP サーバに対し、前記利用者情報入力処理ステップによって入力された利用者識別情報を送信し、前記 LDAP サーバによって前記利用者識別情報に基づいて検索された前記課金情報を受信することを特徴とする。

#### 【0040】

この請求項 16 にかかる発明によれば、外部サーバ通信ステップは、前記利用者識別情報と前記利用者認証情報を管理するインターネット上の LDAP サーバに対し、前記利用者情報入力処理ステップによって入力された利用者識別情報を送信し、前記 LDAP サーバによって前記利用者識別情報に基づいて検索された前記課金情報を受信することで、課金情報の検索時間を短縮することができる。

#### 【0041】

##### 【発明の実施の形態】

以下に添付図面を参照して、この発明にかかる画像形成装置、利用者認証方法および課金処理方法の好適な実施の形態を詳細に説明する。

#### 【0042】

##### (実施の形態 1)

図 1 は、この発明の実施の形態 1 である画像形成装置（以下、「複合機」という。）の主要構成および複合機を含むネットワーク構成を示す説明図である。実施の形態 1 にかかる複合機 100 は、オペレーションパネルにユーザ名、パスワードの入力画面を表示し、入力されたユーザ名でインターネット上の外部サーバにパスワードの問い合わせを行い、入力されたパスワードと外部サーバから取得したパスワードによって利用者認証を行って、利用者のアプリケーションの利用制限を行うものである。

#### 【0043】

図 1 に示すように、本実施の形態にかかる複合機 100 は、インターネット 170 に接続されており、インターネット 170 には LDAP サーバ (Light weigh Directry Access Protocol) 300 が接

続されている。ここで、複合機 100、LDAPサーバ 300間の通信プロトコルはTCP/IPを利用している。

#### 【0044】

本実施の形態の複合機 100において本発明の利用者認証方法を実現するための主要構成としては、図 1に示すように、認証アプリ 117、コピーアプリなどのアプリケーションと、OCS 126、SCS 122、CCS 129などの後述するコントロールサービスと、汎用OSのデーモン（プロセス）として動作するinetd 141およびhttpd 142と、ネットワークコントローラ 103と、オペレーションパネル 150とを主に備えている。

#### 【0045】

LDAPサーバ 300は、X.500ベースのディレクトリサービスをインターネット向けに軽量化したプロトコルに従ってディレクトリサービスを提供するサーバである。LDAPサーバ 300には、ユーザ名に対し、パスワード、メールアドレス、他利用者の個人情報に対応づけられて記憶されている。

#### 【0046】

認証アプリ 117は、LDAPサーバを利用して、ユーザ名とパスワードによって利用者認証処理を行うものである。認証アプリ 117は、利用者情報入力処理部 151と、外部サーバ通信部 152と、認証部 153とから構成される。

#### 【0047】

利用者情報入力処理部 151は、利用者に固有のユーザ名（利用者識別情報）と、利用者の正当性を示すパスワード（利用者認証情報）の要求を行うユーザ名、パスワード入力画面をオペレーションパネル 150の操作表示部に表示し、ユーザ名、パスワードの入力を受け付けるものである。

#### 【0048】

外部サーバ通信部 152は、インターネット 170上のLDAPサーバ 300に対して、オペレーションパネル 150の操作表示部から入力されたユーザIDをLDAPサーバに送信して、複合機 100におけるユーザ名の利用者のパスワードを検索させ、検索結果としてのパスワードを受信するものである。

#### 【0049】

認証部153は、LDAPサーバ300から受信したパスワードとオペレーションパネルの操作表示部から入力されたパスワードが一致しているか否かを判断し、その判断結果（一致、もしくは不一致）を、他のプロセスであるCCS129にプロセス間通信によって送信するものである。

#### 【0050】

CCS (Certification Control Service) 129は、利用者の利用者制限や利用者の課金処理を行うコントロールサービスである。本実施の形態の複合機100では、CCS129は、認証アプリ117117の認証部153から利用者認証の判断結果を受信して、利用者の利用制限をするか否かをコピーアプリ112に送信するようになっている。なお、OCS126、SCS122などのコントロールサービスについては後述する。

#### 【0051】

inetd141は、データの送受信要求を常時監視し、特定のプロトコルに対する接続要求を検出した場合に、それぞれのプロトコルを処理するサーバプログラムを起動するデーモンであり、通常のUNIX（登録商標）におけるinetdと同様の処理が行われる。実施の形態1の複合機100では、httpプロトコルおよびhttpsプロトコルによるデータの送受信のためのポートを常時監視して、かかるポートでの接続要求を検出した場合に、httd142を起動する。

#### 【0052】

httd142は、httpプロトコルおよびhttpsプロトコルで送信されてくるメッセージを受信するポート80番を常時監視しており、このポート80番でリクエストメッセージの受信を行うとともに、レスポンスメッセージの送信を行うものである。なお、リクエストメッセージおよびレスポンスメッセージの構造は、通常のhttpプロトコルにおける各メッセージの構造と同様であり、各メッセージには、html形式で記述されたメッセージボディが含まれている。

#### 【0053】

ネットワークコントローラ103は、httpプロトコル、httpsプロト

コルによる各種データの通信を行うものである。

#### 【0054】

次に、本実施の形態にかかる複合機100の全体の機能的構成について説明する。図2は、実施の形態1の複合機100の全体構成を示すブロック図である。図2に示すように、複合機100は、白黒レーザプリンタ（B&W LP）101と、カラーレーザプリンタ（Color LP）102と、ネットワークコントローラ103と、スキャナ、ファクシミリ、メモリなどのハードウェアリソース104を有するとともに、プラットフォーム120と、アプリケーション130とから構成されるソフトウェア群110とを備えている。

#### 【0055】

プラットフォーム120は、アプリケーションからの処理要求を解釈してハードウェア資源の獲得要求を発生させるコントロールサービスと、一または複数のハードウェア資源の管理を行い、コントロールサービスからの獲得要求を調停するシステムリソースマネージャ（SRM）123と、汎用OS121とを有する。

#### 【0056】

コントロールサービスは、複数のサービスモジュールから形成され、SCS（システムコントロールサービス）122と、ECS（エンジンコントロールサービス）124と、MCS（メモリコントロールサービス）125と、OCS（オペレーションパネルコントロールサービス）126と、FCS（ファックスコントロールサービス）127と、NCS（ネットワークコントロールサービス）128と、CCS（認証コントロールサービス）129から構成される。このプラットフォーム120は、あらかじめ定義された関数により前記アプリケーション130から処理要求を受信可能とするアプリケーションプログラムインタフェース（API）を有する。

#### 【0057】

汎用OS121は、UNIX（登録商標）などの汎用オペレーティングシステムであり、プラットフォーム120並びにアプリケーション130の各ソフトウェアをそれぞれプロセスとして並列実行する。

#### 【0058】

SRM123のプロセスは、SCS122とともにシステムの制御およびリソースの管理を行うものである。SRM123のプロセスは、スキャナ部やプリンタ部などのエンジン、メモリ、HDDファイル、ホストI/O（セントロI/F、ネットワークI/F（ネットワークコントローラ103）、IEEE1394 I/F、RS232C I/Fなど）のハードウェア資源を利用する上位層からの要求にしたがって調停を行い、実行制御する。

#### 【0059】

具体的には、このSRM123は、要求されたハードウェア資源が利用可能であるか（他の要求により利用されていないかどうか）を判断し、利用可能であれば要求されたハードウェア資源が利用可能である旨を上位層に伝える。また、SRM123は、上位層からの要求に対してハードウェア資源の利用スケジューリングを行い、要求内容（例えば、プリンタエンジンにより紙搬送と作像動作、メモリ確保、ファイル生成など）を直接実施している。

#### 【0060】

SCS122のプロセスは、アプリ管理、操作部制御、システム画面表示、LED表示、リソース管理、割り込みアプリ制御などを行う。

#### 【0061】

ECS124のプロセスは、白黒レーザプリンタ（B&W LP）101、カラーレーザプリンタ（Color LP）102、スキャナ、ファクシミリなどからなるハードウェアリソース104のエンジンの制御を行う。

#### 【0062】

MCS125のプロセスは、画像メモリの取得および解放、ハードディスク装置（HDD）の利用、画像データの圧縮および伸張などを行う。

#### 【0063】

FCS127のプロセスは、システムコントローラの各アプリ層からPSTN/I SDN網を利用したファクシミリ送受信、BKM（バックアップSRAM）で管理されている各種ファクシミリデータの登録／引用、ファクシミリ読みとり、ファクシミリ受信印刷、融合送受信を行うためのAPIを提供する。

#### 【0064】



NCS128のプロセスは、ネットワークI/Oを必要とするアプリケーションに対して共通に利用できるサービスを提供するためのプロセスであり、ネットワーク側から各プロトコルによって受信したデータを各アプリケーションに振り分けたり、アプリケーションからデータをネットワーク側に送信する際の仲介を行う。

#### 【0065】

OCS126のプロセスは、オペレータ（ユーザ）と本体制御間の情報伝達手段となるオペレーションパネル（操作パネル）150の制御を行う。OCS126は、オペレーションパネルからキー押下（またはタッチ操作）をキーイベントとして取得し、取得したキーに対応したキーイベント関数をSCS122に送信するOCSプロセスである。また、オペレーションパネル150の操作表示部に対する各種画面を描画出力やその他オペレーションパネルに対する制御は、OCS関数ライブラリに登録されている描画関数等の各種関数をアプリケーション130またはコントロールサービスから呼び出すことにより行われる。このOCS関数ライブラリは、アプリケーション130およびコントロールサービスの各モジュールに動的にリンクされている。なお、OCS126のすべてをプロセスとして動作させるように構成しても良く、あるいはOCS126のすべてをOCS関数ライブラリとして構成しても良い。

#### 【0066】

アプリケーション130は、ページ記述言語（PDL）、PCLおよびポストスクリプト（PS）を有するプリンタ用のアプリケーションであるプリンタアプリ111と、コピー用アプリケーションであるコピーアプリ112と、ファクシミリ用アプリケーションであるファックスアプリ113と、スキャナ用アプリケーションであるスキャナアプリ114と、ネットワークファイル用アプリケーションであるネットファイルアプリ115と、工程検査用アプリケーションである工程検査アプリ116と、上述した認証アプリ117とを有している。

#### 【0067】

アプリケーション130の各プロセス、コントロールサービスの各プロセスは、関数呼び出しとその戻り値送信およびメッセージの送受信によってプロセス間

通信を行いながら、コピー、プリンタ、スキャナ、ファクシミリなどの画像形成処理にかかるユーザサービスを実現している。

#### 【0068】

このように、実施の形態1にかかる複合機100には、複数のアプリケーション130および複数のコントロールサービスが存在し、いずれもプロセスとして動作している。そして、これらの各プロセス内部には、一または複数のスレッドが生成されて、スレッド単位の並列実行が行われる。そして、コントロールサービスがアプリケーション130に対し共通サービスを提供しており、このため、これらの多数のプロセスが並列動作、およびスレッドの並列動作を行って互いにプロセス間通信を行って協調動作をしながら、コピー、プリンタ、スキャナ、ファクシミリなどの画像形成処理にかかるユーザサービスを提供するようになって

#### 【0069】

また、複合機100には、複合機100の顧客、サードベンダなどの第三者がコントロールサービス層の上のアプリケーション層に外部アプリを開発して搭載することが可能となっている。認証アプリ117は、このような外部アプリとして開発されたものであっても良い。

#### 【0070】

なお、実施の形態1にかかる複合機100では、複数のアプリケーション130のプロセスと複数のコントロールサービスのプロセスとが動作しているが、アプリケーション130とコントロールサービスのプロセスがそれぞれ単一の構成とすることも可能である。また、各アプリケーション130は、アプリケーションごとに追加または削除することができる。

#### 【0071】

次に、以上のように構成された実施の形態1にかかる複合機100による利用者認証方法について説明する。図3は、複合機100による利用者認証処理におけるデータの流れを示す説明図であり、図4は、利用者認証処理の手順を示すフローチャートである。

#### 【0072】

本実施の形態の複合機 100 では、電源投入後、まずコピーアプリ 112 が優先的に起動し、その際に利用者認証が行われ、認証結果が正当であれば、コピーアプリ 112 が初期画面をオペレーションパネル 150 の操作表示部 150a に出力し、コピー操作ができるようになっている。

#### 【0073】

まず、認証アプリ 117 の利用者情報入力処理部 151 は、オペレーションパネル 150 の操作表示部 150a に図 5 に示すユーザ名・パスワード入力画面 501 を表示する（ステップ S401）。ここで各種画面の操作表示部 150a への表示は、OCS 関数ライブラリの描画関数呼び出しによって行われる。以下、操作表示部 150a への表示の説明では、描画関数呼び出しを行うことを前提とし、その旨の説明は省略する。また、操作表示部 150a からキー入力を行った場合、入力キーのキーイベントを OCS 126 で取得して、SCS 122 を経由して認証アプリ 117 の利用者情報入力処理部 151 に通知される。

#### 【0074】

ユーザ名・パスワード入力画面 501 からユーザ名、パスワードが入力されたら、認証アプリ 117 の外部サーバ通信部 152 は、入力されたユーザ名およびエントリ検索要求を LDAP サーバ 300 に送信することにより、LDAP サーバ 300 によってユーザ名のエントリの検索を実行させる（ステップ S402）。外部サーバ通信部 152 によるユーザ名およびエントリ検索要求の LDAP サーバ 300 への送信は、inetd 141 が httpd 142 を起動し、httpd 142 からネットワークコントローラ 103 を経由して行われる。また、検索結果は、ネットワークコントローラ 103、httpd 142 を経由して外部サーバ通信部 152 に通知される。

#### 【0075】

ここで、ステップ S402 における外部サーバ通信部 152 による LDAP サーバ 300 に対するエントリ検索要求の処理について説明する。図 6 は、エントリ検索要求処理の手順を示すフローチャートである。

#### 【0076】

外部サーバ通信部 152 は、まず検索フィルタに入力されたユーザ ID を設定

する（ステップS601）。具体的には、例えば「user ID=XXXXXX X」という設定を行う。

#### 【0077】

次に、これからの操作で使用するセッションハンドルを取得するため、ldap\_\_init（）関数を発行する（ステップS602）。セッションハンドルを取得したら、LDAPサーバ300に対する検索関数を実行する。具体的には、接続先LDAPサーバのIPアドレス、接続先ポート、接続権限パスワード、検索位置、ステップS601で設定した検索フィルタ、検索属性（パスワードを指定）をパラメタとして指定して、ldapsearch（）関数を呼び出す（ステップS603）。

#### 【0078】

これにより、LDAPサーバ300で指定されたユーザIDに対応するパスワードが検索され、検索結果として検索されたパスワードがLDAPサーバから受信される（ステップS604）。そして、最後に、セッションハンドルを解放するため、ldap\_\_unbind（）関数を呼び出す（ステップS605）。これにより一連の検索要求処理が完了する。

#### 【0079】

図4に戻り、次に、認証アプリ117の認証部153は、LDAPサーバ300から受信した検索結果としてのパスワードと、ユーザ名・パスワード入力画面501から入力されたパスワードを比較して一致しているか否かを判断する（ステップS403）。そして、一致している場合には、認証結果「一致」をCCS129に送信する（ステップS404）。一方、両パスワードが一致していない場合には、認証結果「不一致」をCCS129に送信する（ステップS405）。

#### 【0080】

認証結果を受信したCCS129は、認証結果が「一致」か否かを判断する（ステップS406）。そして、「一致」である場合には、正当な利用者であると判断しコピーアプリ112の利用制限を行わない。この場合、CCS129は、コピーアプリ112に対し、初期画面の表示要求を行う（ステップS407）。

初期画面の表示要求を受けたコピーアプリ 1 1 2 は、オペレーションパネル 1 5 0 の操作表示部 1 5 0 a に初期画面を表示する（ステップ S 4 0 8）。

#### 【0 0 8 1】

一方、「不一致」である場合には、CCS 1 2 9 は、オペレーションパネル 1 5 0 の操作表示部 1 5 0 a にコピーアプリの利用が制限される旨のエラーメッセージを表示する（ステップ S 4 0 9）。これによって、利用者認証および利用制限の処理が完了する。

#### 【0 0 8 2】

このように実施の形態 1 にかかる複合機 1 0 0 では、認証アプリ 1 1 7 の利用者情報入力処理部 1 5 1 によって、利用者に固有のユーザ ID とパスワードを入力させ、外部サーバ通信部 1 5 2 によって、インターネット 1 7 0 に接続された LDAP サーバ 3 0 0 に対し入力されたユーザを送信し、LDAP サーバ 3 0 0 によって検索されたパスワードを受信し、認証部 1 5 3 によって、外部サーバ通信部 1 5 2 によって受信したパスワードと、利用者情報入力処理部 1 5 1 によって入力されたパスワードとが一致するか否かを判断し、判断結果を、CCS 1 2 9 に通知しているので、自己の複合機内に認証データベースを保持する必要がなくなり、認証データベースのメンテナンス作業の労力を軽減することができる。また、各複合機 1 0 0 に認証データベースを保持する必要がないため、パスワードなどの情報の改ざんを防止することができ、複合機 1 0 0 のセキュリティの強化を図ることができる。

#### 【0 0 8 3】

##### （実施の形態 2）

実施の形態 1 にかかる複合機 1 0 0 は、オペレーションパネルにユーザ名、パスワードの入力画面を表示し、入力されたユーザ名でインターネット上の外部サーバにパスワードの問い合わせを行うものであったが、この実施の形態 2 にかかる複合機 7 0 0 は、インターネット上の PC 2 0 0 からユーザ名と課金データを受信して外部サーバに課金データの問い合わせを行うものである。

#### 【0 0 8 4】

図 7 は、実施の形態 2 にかかる複合機 7 0 0 の主要構成および複合機を含むネ

ネットワーク構成を示す説明図である。図8は、実施の形態2の複合機700の全体の機能的構成を示すブロック図である。

#### 【0085】

図7に示すように、本実施の形態にかかる複合機700も、インターネット170に接続されており、インターネット170にはLDAPサーバ(Light weigh Directry Access Protocol)300とクライアント端末としてのPC(Personal Computer)が接続されている。ここで、複合機100、LDAPサーバ300およびPC200間の通信プロトコルはTCP/IPを利用している。

#### 【0086】

本実施の形態の複合機700において本発明の課金処理方法を実現するための主要構成としては、図7に示すように、課金アプリ717、コピーアプリなどのアプリケーションと、OCS126、SCS122、CCS129、NCS126などの後述するコントロールサービスと、汎用OSのデーモン(プロセス)として動作するinetd141およびhttpd142と、ネットワークコントローラ103と、オペレーションパネル150とを主に備えている。

#### 【0087】

本実施の形態のLDAPサーバ300は、ユーザ名に対し、パスワード、メールアドレスの他、課金データが対応づけられて記憶されている。課金データとしては、予算(使用可能金額)、A4使用可能枚数、B5使用可能枚数などがある。

#### 【0088】

本実施の形態のPC200には、ICカードのリード制御を行うICカードリーダー201が接続されている。このICカードリーダー201に、ユーザ名、課金データが記録されたICカードを読み込ませ、ユーザ名、課金データをPC200から複合機700に送信するようになっている。ICカードに記録されている課金データとしては、使用金額、A4使用枚数、B5使用枚数などである。

#### 【0089】

複合機700における課金アプリ717は、LDAPサーバ300を利用して

、ユーザ名と課金データによって課金処理を行うものである。課金アプリ 717 は、利用者情報受信部 751 と、外部サーバ通信部 752 と、課金処理部 753 とから構成される。

#### 【0090】

利用者情報入力処理部 151 は、ユーザ名（利用者識別情報）と、パスワードを IC カードから読みとった PC 200 から受信するものである。

#### 【0091】

外部サーバ通信部 152 は、インターネット 170 上の LDAP サーバ 300 に対して、オペレーションパネル 150 の操作表示部から入力されたユーザ ID を LDAP サーバに送信して、複合機 100 におけるユーザ名の利用者の課金データを検索させ、検索結果としての課金データを受信するものである。

#### 【0092】

課金処理部 753 は、LDAP サーバ 300 から受信した課金データと PC 200 から受信した課金データを比較して、利用者の課金データが使用可能な範囲内か否かを判断し、その判断結果（範囲内、もしくは範囲外）を、他のプロセスである CCS 129 にプロセス間通信によって送信するものである。

#### 【0093】

CCS (Certification Control Service) 129 は、利用者の利用者制限や利用者の課金処理を行うコントロールサービスである。本実施の形態の複合機 700 では、CCS 129 は、課金アプリ 717 の課金処理部 753 から課金処理の判断結果を受信して、利用者の利用制限をするか否かをコピーアプリ 112 に送信するようになっている。複合機 700 のその他の構成については、実施の形態 1 の複合機 100 と同様である。

#### 【0094】

次に、以上のように構成された実施の形態 2 にかかる複合機 700 による課金処理および課金に基づく利用制限処理について説明する。図 9 は、複合機 700 による課金処理および課金に基づく利用制限処理におけるデータの流れを示す説明図であり、図 10 は、課金処理および課金に基づく利用制限処理の手順を示すフローチャートである。

## 【0095】

本実施の形態の複合機700では、インターネット170上のPC200からユーザ名、課金データを受信したときに、イベントドリブンで課金アプリ717が実行されるようになっている。そして、課金処理が行われ処理結果が正当であれば、コピーアプリ112が初期画面をオペレーションパネル150の操作表示部150aに出力し、コピー操作ができるようになっている。

## 【0096】

課金アプリ717は、その利用者情報受信部751によってPC200からユーザ名、課金データを受信する。より具体的には、PC200によって送信されたユーザ名および課金データは、複合機700のネットワークコントローラ103で受信され、NCSS128を経由して利用者情報受信部751で受信する。そして、外部サーバ通信部152は、受信したユーザ名およびエントリ検索要求をLDAPサーバ300に送信することにより、LDAPサーバ300によってユーザ名のエントリの検索を実行させる（ステップS1001）。外部サーバ通信部752によるLDAPサーバ300に対するエントリ検索要求の処理については、実施の形態1の複合機100と同様である。ただし、検索属性としては「課金データ」を設定して、`ldapsearch()`関数を呼び出すものとする。

## 【0097】

次に、課金アプリ717の課金処理部753は、LDAPサーバ300から受信した検索結果としての課金データと、PC200から受信した課金データを比較して、PC200から受信した課金データが複合機700の利用可能な範囲内か否かを判断する（ステップS1002）。そして、範囲内である場合には、処理結果「範囲内」をCCSS129に送信する（ステップS1003）。一方、範囲外である場合には、処理結果「範囲外」をCCSS129に送信する（ステップS1004）。

## 【0098】

処理結果を受信したCCSS129は、処理結果が「範囲内」か否かを判断する（ステップS1005）。例えば、使用金額が予算未満か否か、用紙の使用枚数が使用枚数未満か否かを判断する。そして、「範囲内」である場合には、利用者



は複合機 700 をまだ使用できると判断しコピーアプリ 112 の利用制限を行わない。この場合、CCS 129 は、コピーアプリ 112 に対し、初期画面の表示要求を行う（ステップ S1006）。初期画面の表示要求を受けたコピーアプリ 112 は、オペレーションパネル 150 の操作表示部 150a に初期画面を表示する（ステップ S1007）。

#### 【0099】

一方、ステップ S1005 において、「範囲外」と判断された場合には、CCS 129 は、オペレーションパネル 150 の操作表示部 150a にコピーアプリ 112 の利用が制限される旨のエラーメッセージを表示する（ステップ S1008）。これによって、課金処理および利用制限の処理が完了する。

#### 【0100】

このように実施の形態 2 にかかる複合機 700 では、認証アプリ 717 の利用者情報受信部 751 によって、インターネット 170 上の PC 200 からユーザ ID と課金データを受信し、外部サーバ通信部 752 によって、インターネット 170 に接続された LDAP サーバ 300 に対し入力されたユーザを送信し、LDAP サーバ 300 によって検索された課金データを受信し、課金処理部 753 によって、外部サーバ通信部 152 によって受信した課金データと、利用者情報受信部 751 によって受信した課金データとを比較し、その比較結果を、CCS 129 に通知しているので、自己の複合機内に課金データベースを保持する必要がなくなり、課金データベースのメンテナンス作業の労力を軽減することができる。また、各複合機 700 に課金データベースを保持する必要がないため、課金データなどの情報の改ざんを防止することができ、複合機 700 のセキュリティの強化を図ることができる。

#### 【0101】

##### 【発明の効果】

以上説明したように、請求項 1 にかかる発明によれば、外部サーバで利用者識別情報と利用者認証情報とを一括管理するので、自己の画像形成装置内に利用者識別情報と利用者認証情報とを対応づけた認証データベースを保持する必要がなくなり、認証データベースのメンテナンス作業の労力を軽減できると

いう効果を奏する。また、各画像形成装置に認証データベースを保持する必要がないため、利用者認証情報の改ざんを防止することができ、画像形成装置のセキュリティの強化を図ることができるという効果を奏する。

【0102】

また、請求項2にかかる発明によれば、認証データベースのメンテナンス作業の労力の軽減を図りつつ、利用者認証情報に基づく画像形成装置の利用制限によるセキュリティ強化を向上させることができるという効果を奏する。

【0103】

また、請求項3にかかる発明によれば、利用者認証情報の検索時間を短縮することができるという効果を奏する。

【0104】

また、請求項4にかかる発明によれば、認証アプリをはじめとするアプリケーションのソフトウェア開発において、ユーザサービスに固有の部分だけで行うことができ、ソフトウェア開発の労力軽減を図ることができるという効果を奏する。

【0105】

また、請求項5にかかる発明によれば、外部サーバで利用者識別情報と課金情報とを一括管理するので、自己の画像形成装置内に利用者識別情報と課金情報とを対応づけた課金データベースを保持する必要がなくなり、課金データベースのメンテナンス作業の労力を軽減することができるという効果を奏する。また、各画像形成装置に課金データベースを保持する必要がないため、課金情報の改ざんを防止することができ、画像形成装置のセキュリティの強化を図ることができるという効果を奏する。

【0106】

また、請求項6にかかる発明によれば、課金データベースのメンテナンス作業の労力の軽減を図りつつ、課金情報に基づく画像形成装置の利用制限によるセキュリティ強化を向上させることができるという効果を奏する。

【0107】

また、請求項7にかかる発明によれば、任意の外部記憶媒体に記録した課金情

報に基づく利用制限を行うことができ、利用者の便宜が図られるという効果を奏する。

【0108】

また、請求項 8 にかかる発明によれば、課金情報の検索時間を短縮することができるという効果を奏する。

【0109】

また、請求項 9 にかかる発明によれば、課金アプリをはじめとするアプリケーションのソフトウェア開発において、ユーザサービスに固有の部分だけで行うことができ、ソフトウェア開発の労力軽減を図ることができるという効果を奏する。

【0110】

また、請求項 10 にかかる発明によれば、外部サーバで利用者識別情報と利用者認証情報とを一括管理するので、自己の画像形成装置内に利用者識別情報と利用者認証情報とを対応づけた認証データベースを保持する必要がなくなり、認証データベースのメンテナンス作業の労力を軽減することができるという効果を奏する。また、各画像形成装置に認証データベースを保持する必要がないため、利用者認証情報の改ざんを防止ことができ、画像形成装置のセキュリティの強化を図ることができるという効果を奏する。

【0111】

また、請求項 11 にかかる発明によれば、認証データベースのメンテナンス作業の労力の軽減を図りつつ、利用者認証情報に基づく画像形成装置の利用制限によるセキュリティ強化を向上させることができるという効果を奏する。

【0112】

また、請求項 12 にかかる発明によれば、利用者認証情報の検索時間を短縮することができるという効果を奏する。

【0113】

また、請求項 13 にかかる発明によれば、外部サーバで利用者識別情報と課金情報とを一括管理するので、自己の画像形成装置内に利用者識別情報と課金情報とを対応づけた課金データベースを保持する必要がなくなり、課金データベース

のメンテナンス作業の労力を軽減することができるという効果を奏する。また、各画像形成装置に課金データベースを保持する必要がないため、課金情報の改ざんを防止することができ、画像形成装置のセキュリティの強化を図ることができるという効果を奏する。

**【0114】**

また、請求項14にかかる発明によれば、課金データベースのメンテナンス作業の労力の軽減を図りつつ、課金情報に基づく画像形成装置の利用制限によるセキュリティ強化を向上させることができるという効果を奏する。

**【0115】**

また、請求項15にかかる発明によれば、任意の外部記憶媒体に記録した課金情報に基づく利用制限を行うことができ、利用者の便宜が図られるという効果を奏する。

**【0116】**

また、請求項16にかかる発明によれば、課金情報の検索時間を短縮することができるという効果を奏する。

**【図面の簡単な説明】**

**【図1】**

実施の形態1にかかる複合機の主要構成および複合機を含むネットワーク構成を示す説明図である。

**【図2】**

実施の形態1の複合機の全体構成を示すブロック図である。

**【図3】**

複合機による利用者認証処理におけるデータの流れを示す説明図である。

**【図4】**

利用者認証処理の手順を示すフローチャートである。

**【図5】**

ユーザ名・パスワード入力画面を示す説明図である。

**【図6】**

エントリ検索要求処理の手順を示すフローチャートである。

**【図 7】**

実施の形態 2 にかかる複合機の主要構成および複合機を含むネットワーク構成を示す説明図である。

**【図 8】**

実施の形態 2 の複合機の全体の機能的構成を示すブロック図である。

**【図 9】**

複合機による課金処理および課金に基づく利用制限処理におけるデータの流れを示す説明図である。

**【図 10】**

課金処理および課金に基づく利用制限処理の手順を示すフローチャートである。

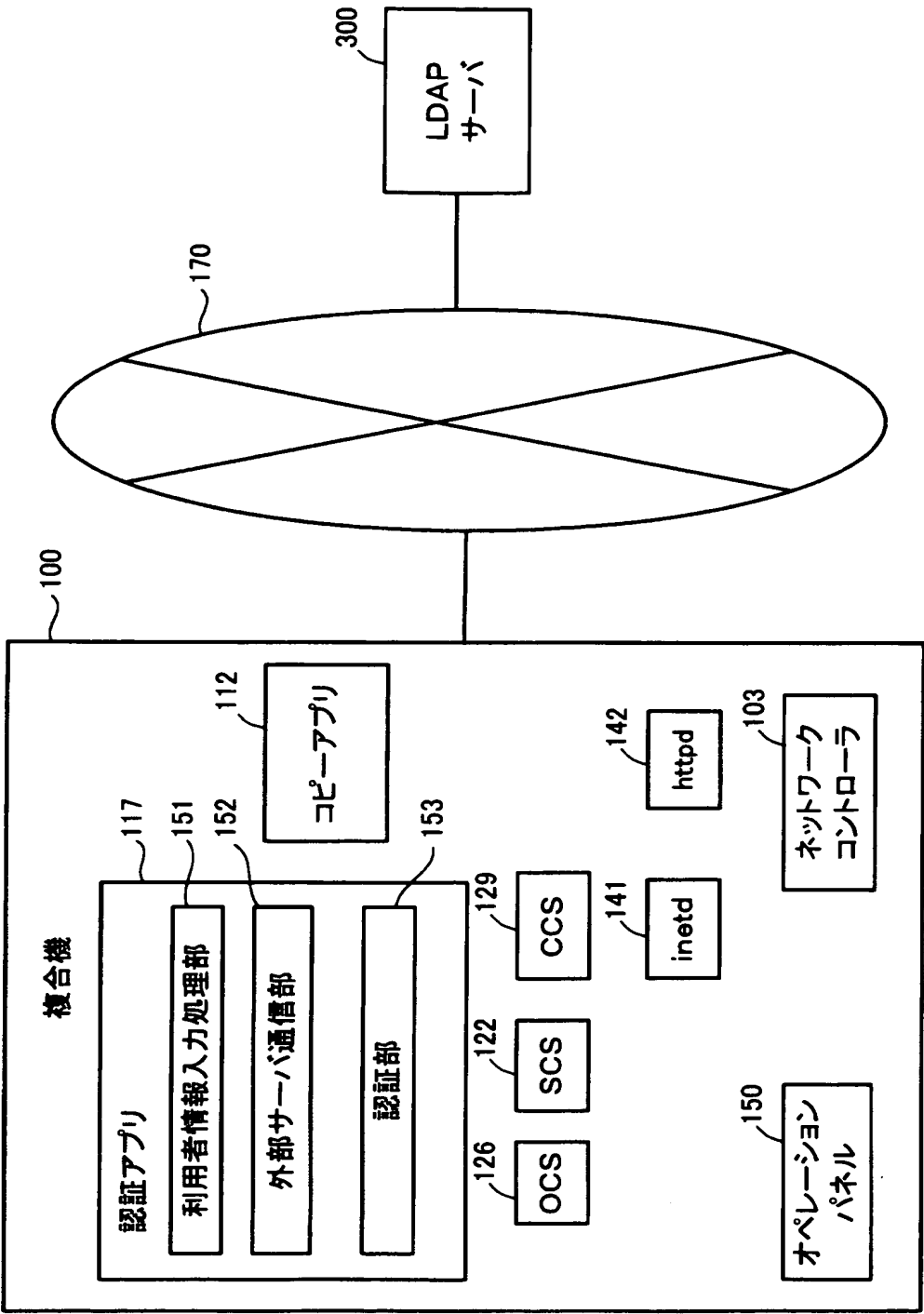
**【符号の説明】**

- 100, 700 複合機
- 101 白黒レーザプリンタ
- 102 カラーレーザプリンタ
- 103 ネットワークコントローラ
- 104 ハードウェアリソース
- 110 ソフトウェア群
- 111 プリンタアプリ
- 112 コピーアプリ
- 113 ファックスアプリ
- 114 スキャナアプリ
- 115 ネットファイルアプリ
- 116 工程検査アプリ
- 117 認証アプリ
- 717 課金アプリ
- 120 プラットホーム
- 121 汎用 OS
- 122 SCS

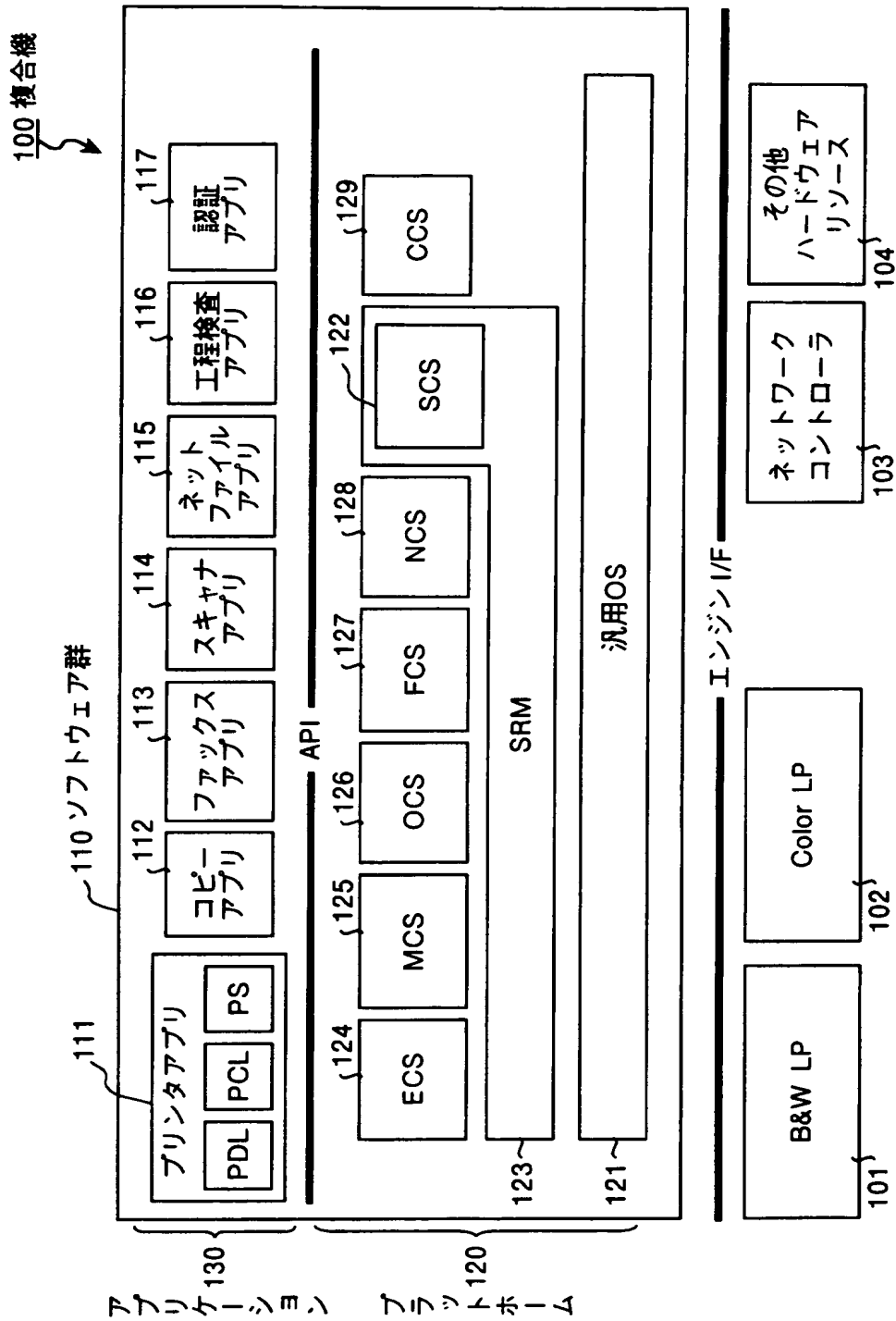
1 2 3 S R M  
1 2 4 E C S  
1 2 5 M C S  
1 2 6 O C S  
1 2 7 F C S  
1 2 8 N C S  
1 2 9 C C S  
1 3 0 アプリケーション  
1 5 0 オペレーションパネル  
1 5 0 a 操作表示部  
1 5 1 利用情報入力処理部  
1 5 2, 7 5 2 外部サーバ通信部  
1 5 3 認証部  
1 7 0 インターネット  
2 0 0 P C  
2 0 1 I C カードリーダー  
3 0 0 L D A P サーバ  
5 0 1 ユーザ I D / パスワード入力画面  
7 5 1 利用情報受信部  
7 5 3 課金処理部

【書類名】 図面

【図 1】

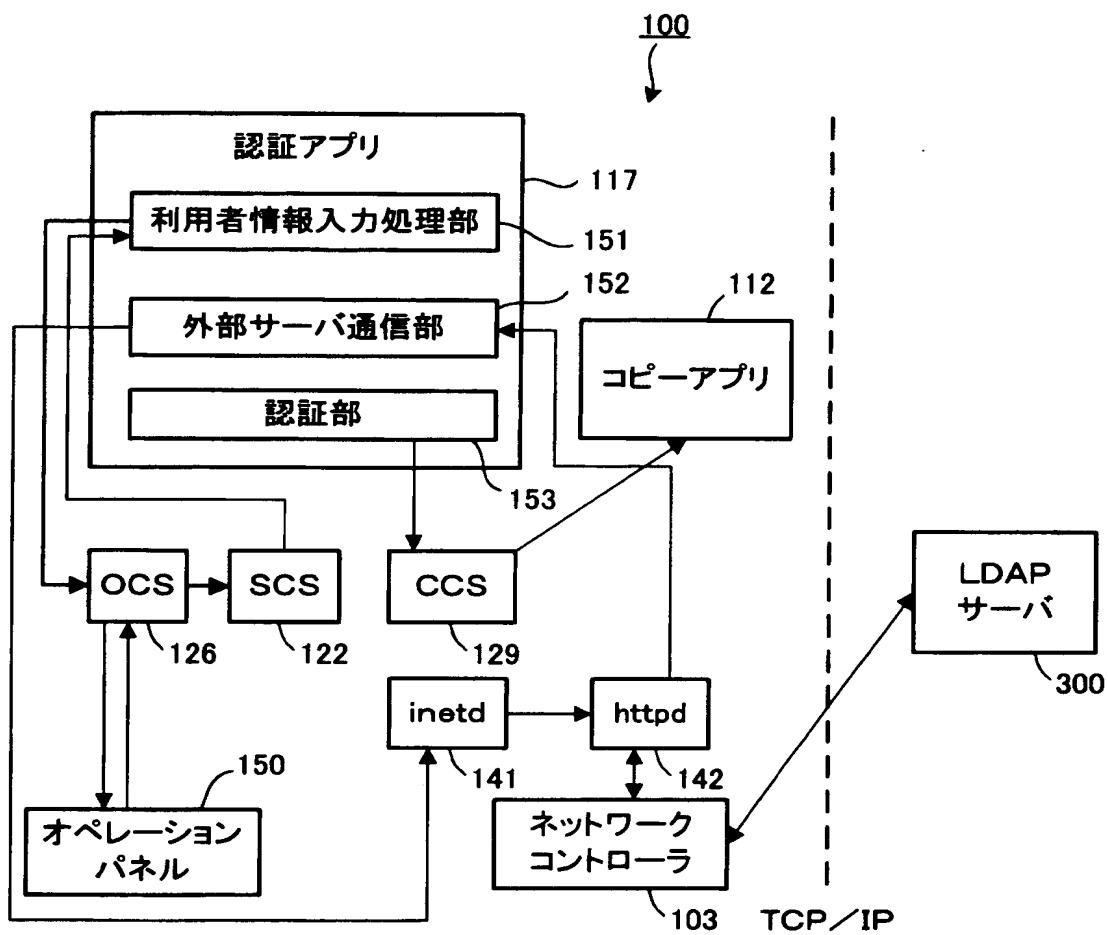


【図 2】

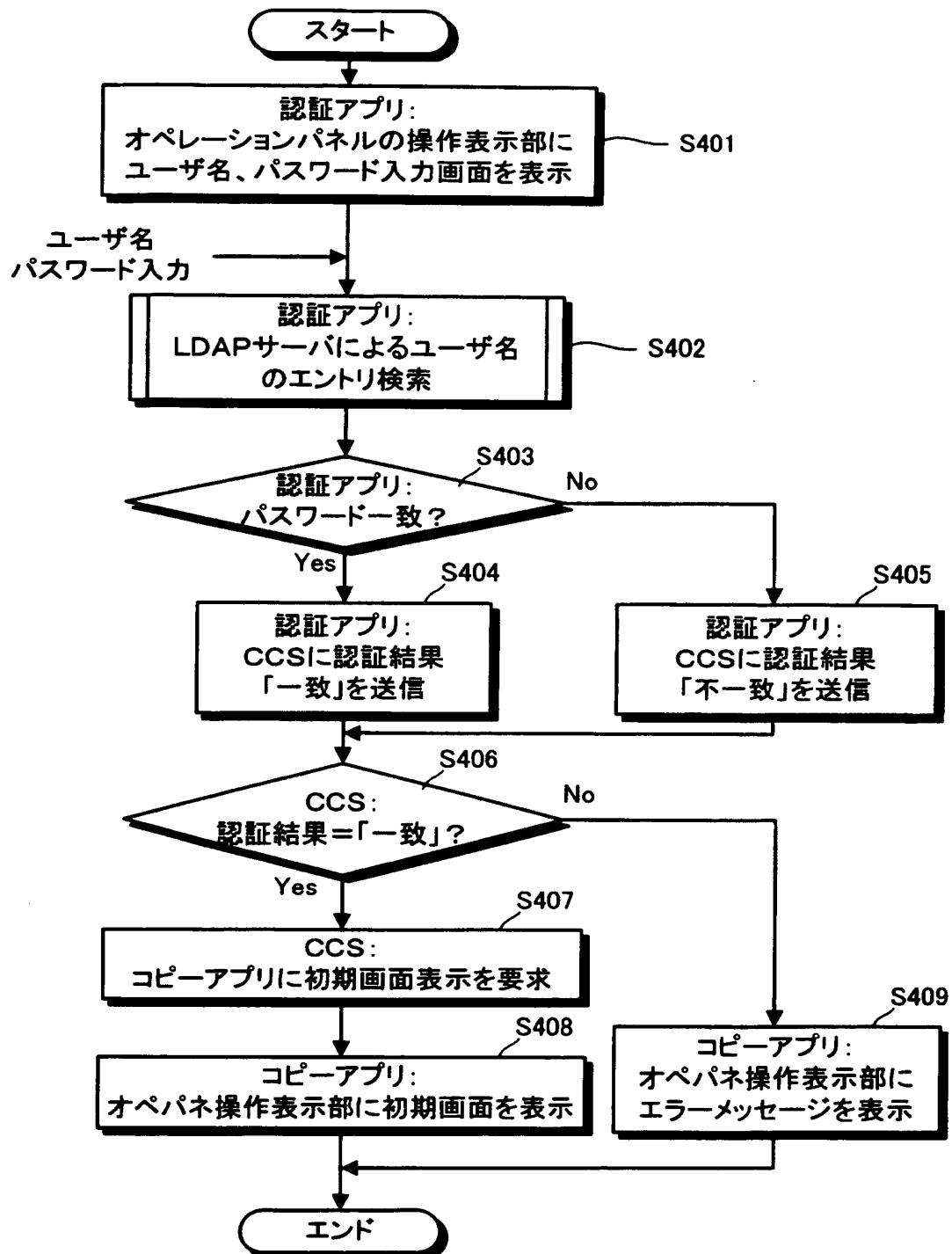




【図 3】



【図 4】



【図 5】

150a

コピー

スキャナ

ファクシミリ

ユーザ名・パスワード入力

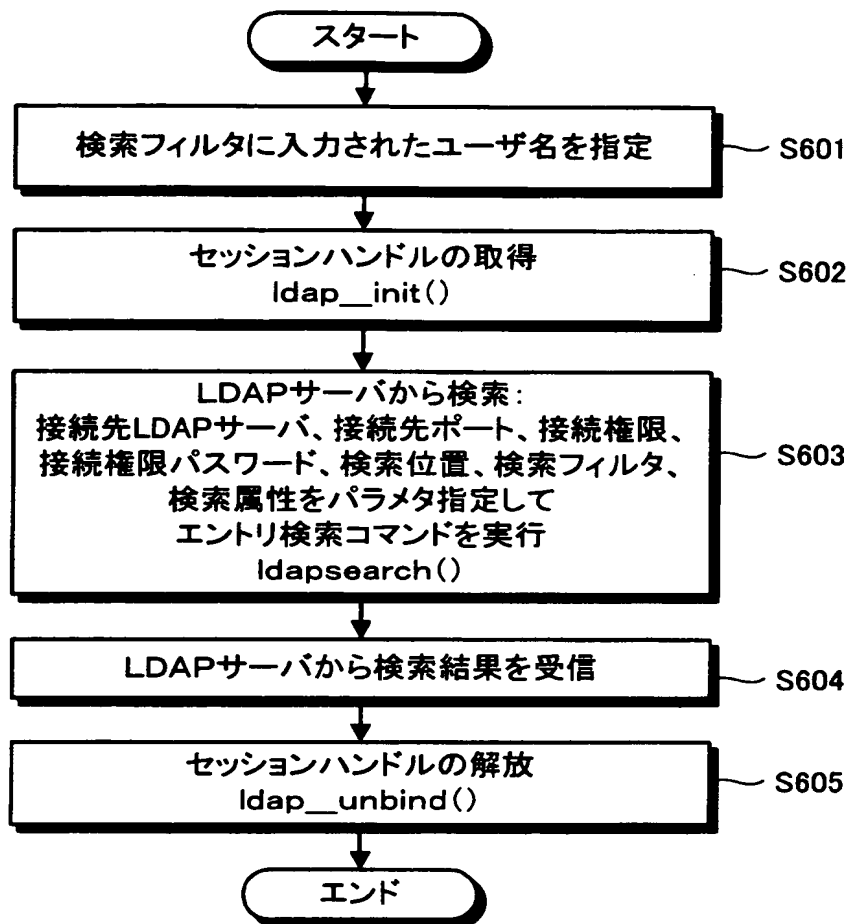
ユーザID:

パスワード:

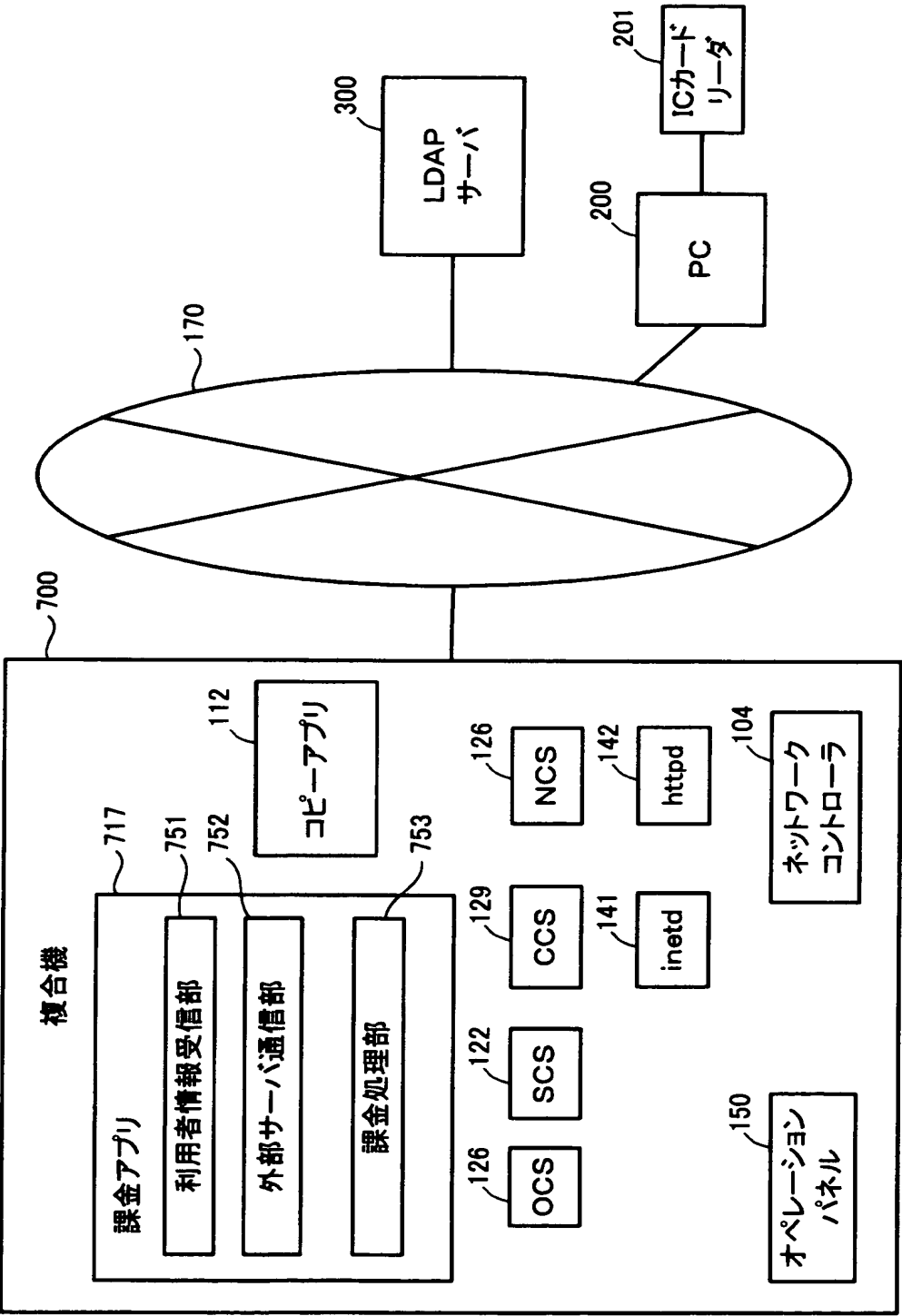
OK キャンセル

501

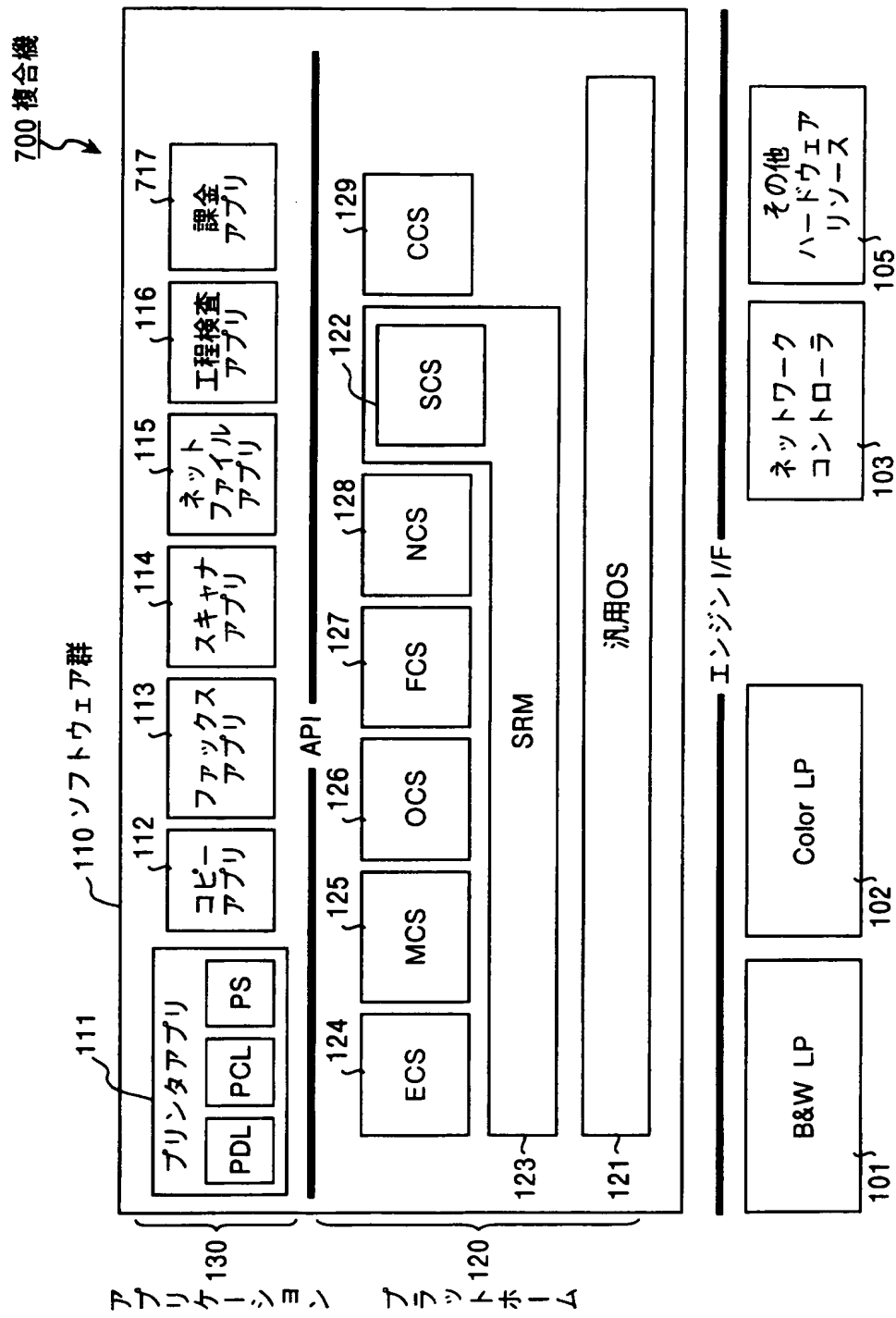
【図 6】



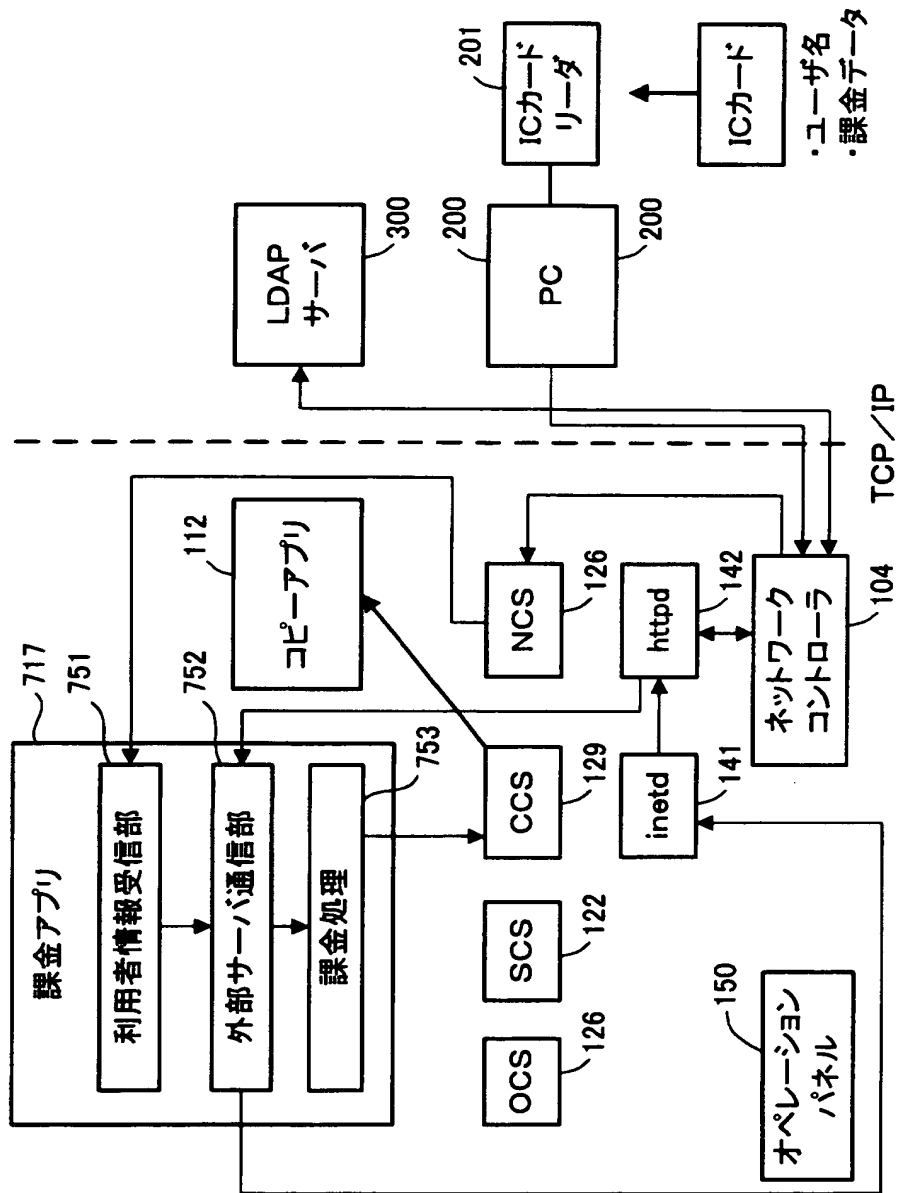
【図 7】



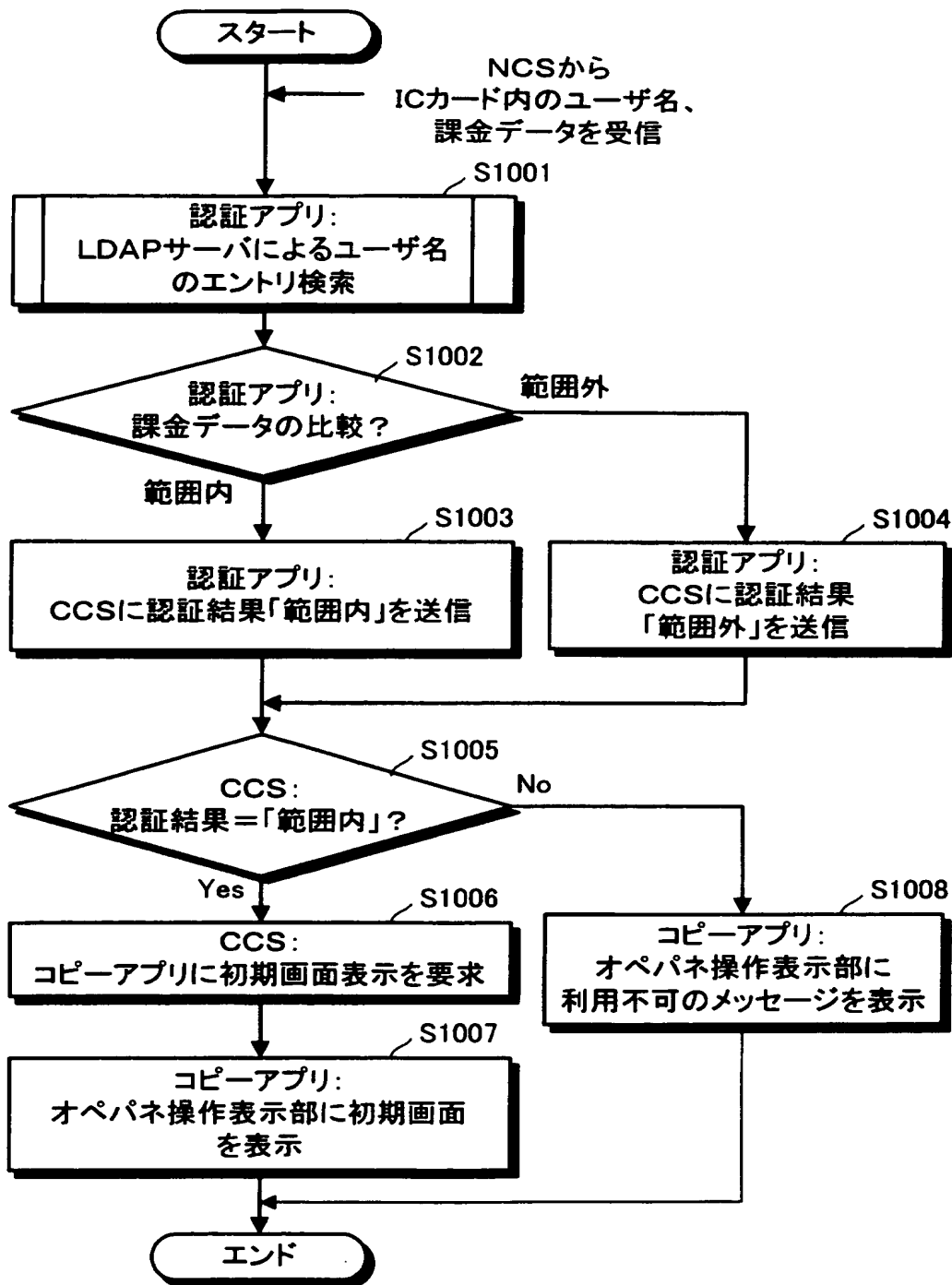
【図 8】



【図 9】



【図10】





【書類名】 要約書

【要約】

【課題】 利用者情報のメンテナンス作業の労力を軽減するとともに、利用者情報のセキュリティの強化を図ること。

【解決手段】 画像形成処理にかかるユーザサービスを提供する画像形成装置であって、利用者に固有のユーザIDと、利用者の正当性を示すパスワードを入力させる利用者情報入力処理部151と、インターネット170に接続され、ユーザIDとパスワードを管理するLDAPサーバ300に対し、ユーザIDを送信し、LDAPサーバ300によって検索されたパスワードを受信する外部サーバ通信部152と、外部サーバ通信部152によって受信したパスワードと、利用者情報入力処理部151によって入力されたパスワードとが一致するか否かを判断し、判断結果を、画像形成装置で動作するCCS129に通知する認証部153とからなる認証アプリ117を備えた。

【選択図】 図1

特願 2 0 0 2 - 2 6 9 2 8 5

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 6 7 4 7 ]

1. 変更年月日

1 9 9 0 年 8 月 2 4 日

[変更理由]

新規登録

住 所

東京都大田区中馬込 1 丁目 3 番 6 号

氏 名

株式会社リコー

2. 変更年月日

2 0 0 2 年 5 月 1 7 日

[変更理由]

住所変更

住 所

東京都大田区中馬込 1 丁目 3 番 6 号

氏 名

株式会社リコー